Establishing a State Cyber Crimes Unit
White Paper

Utah Department of Public Safety
Commissioner Keith Squires
Deputy Commissioner Jeff Carr
Major Brian Redd
Utah Statewide Information & Analysis Center (SIAC)

September 11, 2014
Salt Lake City, Utah

Establishing a State Cyber Crimes Unit

The Growing Cyber Crime Problem

An excerpt from the 12th Annual Cybercrime Trends report states, "The US Director of National Intelligence has ranked cybercrime as the top national security threat." Considering the level to which cyber infrastructure is integrated into every aspect of daily life, it is no wonder that cyber security has become such a concern.

The State of Utah recognized the need to protect its citizens and organizations by taking action on the issue of cyber security. In 2012, Utah experienced a breach of a Utah Medicaid server. Over 780,000 Utah citizens had their personal identifiable information exposed, resulting in legal fees, investigations, and recovery costs of 3.4 million dollars. Due to this breach, as well as other cyber events, including a breach of a police website and cyber criminals exposing personal information of a state legislator over proposed legislation, the State of Utah developed the Utah Statewide Cyber Intelligence Network (USCIN).

The USCIN network is a partnership designed to support investigations, increase resiliency, improve situational awareness, and disrupt cyber crime while working collaboratively with the FBI's Cyber Taskforce to coordinate and deconflict cyber cases. Utah is also advocating for a nationwide network of state and local cyber investigators able to address cyber crime including network intrusion, electronic data theft, unauthorized wire transfers, distributed denial of service attacks, high-level internet fraud, electronic terroristic threats, and other cyber-related crime.

Funding and Support for Cyber Crime Unit

Utah DPS made early efforts to educate the Utah legislature on cyber threats directly affecting Utah and its' citizens and businesses. The Department also shared what efforts were already underway to address those threats.

Utah's Cyber Unit is a result of the efforts of Utah Governor Gary Herbert, Utah Department of Public Safety Commissioner Keith Squires, and the 2013 Utah legislature, including key legislator Eric Hutchings, Kearns Utah. Funding for personnel (three investigators and one analyst), training, and equipment was provided during the 2013 legislative session.

Partnerships

The USCIN utilizes partners from several disciplines to accomplish its' mission including various divisions within the Utah Department of Public Safety, Federal Bureau of Investigation, Department of Homeland Security, the private sector, and local government (see Appendix A).

Statewide Information and Analysis Center (SIAC). The SIAC is Utah's fusion center. The SIAC provides analytical support to local law enforcement and program partners. The SIAC

operates as the coordinator of the Utah Statewide Cyber Intelligence Network (USCIN); integrating data from various sources, maintaining connections with program members, and assisting with case data for cyber investigations and intelligence. The SIAC determines the appropriate use of data through a pre-determined workflow to ensure the efficient and effective use of data (see Appendix B). Utah's cyber analyst is housed in the SIAC.

Utah Department of Technology Services (DTS). DTS provides centralized information technology resources for the vast majority of Utah state agencies and departments. Additionally, DTS provides infrastructure and connectivity for many of Utah's municipalities. DTS assists USCIN with threat intelligence, network trends, and as subject matter experts. As a USCIN member, DTS also receives information contributed by other members that may provide situational awareness or evidence of new attack vectors.

State Bureau of Investigation (SBI). SBI is USCIN's primary point of contact for criminal activity and investigations. As members of the National Cybercrime Investigative Joint Task Force (NCIJTF), SBI works closely with the SIAC and the FBI to investigate cyber related crime in Utah. SBI participates in the USCIN by reviewing and investigating criminal incidents.

State Crime Lab. The State Crime Lab forensics agent assigned to the Regional Computer Forensics Laboratory (RCFL) is also a partner in USCIN. The forensic agent is responsible for the proper collection, handling, and imaging of all computer evidence.

Federal Bureau of Investigation (FBI). The FBI participates in the USCIN by providing valuable high-level intelligence and case vetting. The FBI coordinates the SIAC and SBI's involvement in the NCIJTF, allowing Utah to obtain information for its own cases as well as provide support for the intelligence community. This relationship also provides SBI with multi-jurisdictional authority, increasing their ability to investigate cyber crimes. The FBI also provides the DPS Cyber Unit personnel with Top Secret security clearances, training, and other resources.

Department of Homeland Security (DHS). DHS provides support to the USCIN through partnerships with owners and operators of critical infrastructure such as financial systems, chemical plants, and water and electric utilities; the release of actionable cyber alerts; investigations of cyber criminals involved in financial transaction fraud; and education about how the public can stay safe online.

Private Sector and Local Government. The private sector and local government entities participate in the USCIN by providing the eyes and ears for cyber attacks. These entities provide a significant amount of visibility into the cyber landscape. The USCIN's private and public sector members contribute information about their own networks as well as receive intelligence reports produced by the USCIN.

Cyber Crimes Below Traditional FBI Thresholds

Utah Public Safety Commissioner Keith Squires indicated in a 2014 Police Chief magazine article that the "rapid increase and expansion of cyber related criminal activity inundated FBI Regional Cyber Task Forces with numerous investigative requests, and consequently

(due to limited resources), the minimum threshold for investigative action by the FBI has increased. As a result, many states and localities have begun to include cyber related investigations as a part of their investigative strategies[1]."

At a recent cyber security conference with the private sector, FBI Director James Comey said, "We are working side-by-side with our federal, state, and local partners on Cyber Task Forces in each of our field offices. And we are training our state and local counterparts to triage local cyber matters so that we can focus on national security issues."[2]

Utah Department of Public Safety/Federal Bureau of Investigation Partnership (Operation Well Spring)

The creation of the DPS Cyber Unit is a multiple year process. One of the first initiatives was the formation of a partnership between the Utah Department of Public Safety (DPS) and the Federal Bureau of Investigation (FBI).

Utah DPS recognized early on in the process that due to the international scope of the cyber crime problem, the Department was incapable of effectively dealing with criminals outside the United States. The FBI recognized its' inability to effectively investigate all cyber crimes referred due to resource constraints. Both entities recognized a partnership would leverage finite resources so citizens, businesses, and government agencies affected by cyber crime would have redress.

The first year of the partnership was dedicated to establishing roles and responsibilities, building relationships, providing and obtaining security clearances for state agents, and identifying and participating in training exercises.

In addition to the focus on building the structure, state agents now assigned at the Cyber Task Force within the Salt Lake Division of the FBI, also received an immediate caseload from the FBI's Internet Crime Complaint Center[3] in a partnership known as Operation Well Spring.[4] State agents received approximately 25 cases for review involving over 900 victims, and 2.5 million dollars in loss.

Operation Wells Spring was designed to test the following four concepts:

---

[1] Keith D. Squires, "Cybercrimes Enforcement: A State Perspective," The Police Chief (February 2014): 42–45.

[2] James B. Comey, Director, FBI, RSA Cyber Security Conference, San Francisco, CA, February 26, 2014

[3] The IC3 complaint database contains over three million complaints filed by victims of Internet fraud, computer intrusion, and other web-based crimes. IC3 analysts use this data to create intelligence packages targeting threats to a particular jurisdiction.

[4] In August 2013, the Internet Crimes Complaint Center (IC3), located in Fairmont, WV, launched the Wellspring initiative to create a national platform for the investigation of Internet Crime. The hope was to first leverage state and local law enforcement partners to investigate Internet-enabled crimes, and second to elevate IC3's cyber-security posture and investigative capabilities.

(1) The aggregation of reporting of Internet enabled crime in a central location—the Internet Crimes Complaint Center (IC3)—since Internet-enabled crime crosses local, state, and national boundaries.

(2) The analysis of patterns and trends identifying active and prolific suspects and the preparation of investigative packets for investigators working Operation Well Spring.

(3) The prioritization of investigative leads based upon the likelihood of identifying suspects, disrupting criminal activity through actionable intelligence, and/or successful prosecution.

(4) The effective coordination, communication, and deconfliction of these cases with the FBI Cyber Crimes Taskforce.

Successes, Challenges and Lessons Learned

To date the results of Operation Well Spring are encouraging. Utah DPS has determined IC3.gov is the best point of submission by citizen victims and local law enforcement for Internet or cyber-related crime reporting. Using IC3 will reduce duplication of effort, reduce confusion, and strengthen efforts through the aggregation of data. The challenge now is creating and funding a public awareness campaign and working with local law enforcement to identify ways to increase use while keeping expectations of citizen realistic.

In addition to IC3 referrals, state agents are beginning to receive case referrals from local agencies, the private sector, the Utah Department of Technology Services, and the Salt Lake Division of FBI involving network intrusion, electronic data theft, unauthorized wire transfers, distributed denial of service attacks, electronic terroristic threats, and other cyber-related crime.

Some of the successes Utah has recognized include specialized training of personnel, coordination of scarce resources at all levels, and a formalized structure to address cyber crime. Utah has also had some success addressing cyber fraud including making international arrests through the Cyber Task Force.

To date, the U.S. Attorney's Office in Salt Lake City has willingly worked with state agents on Operation Well Spring cases not generally prosecuted at the federal level. This cooperation has allowed the Cyber Unit to progress quickly.

Utah DPS and the FBI also held meetings early on with key local and state prosecutors in an effort to educate and gain cooperation. The meetings were positive, but more needs to be done. Efforts are being made to strengthen relationships and identify relevant training for prosecutors. In the end, the Utah DPS Cyber Unit would like an embedded prosecutor from the Utah Attorney General's Office due to technical aspects of prosecuting cyber crime.

Lessons learned also include understanding that the definition of success in cyber cases may mean identification, notification, disruption, or mitigation in some cases rather than simply arrest and prosecution. A tremendous amount of pre-case work is needed simply to determine whether or not a crime and/or suspect can be identified. The importance of training prosecutors and understanding the difficulty of placing a suspect behind the computer or intrusion can be a challenge. The anonymity with which cyber crime is

conducted creates tremendous challenges. It has been very clear that a partnership with the FBI and other federal agencies is essential to a successful state cyber program.

Lastly, a model similar to the High Intensity Drug Trafficking Area (HIDTA) initiative[5] should be considered going forward. The HIDTA model facilitates state-to-state coordination of investigations and encourages equal partnerships between local, state, and federal investigative agencies. A similar model must be employed to effectively address cyber crime.

Year Two and Beyond

In year two, USCIN will continue to build intelligence and information sharing capability. The training of cyber investigators and analysts will continue and more focus will be placed on the State of Utah Network. Further development of the relationship between the fusion center (SIAC) and Utah's Department of Technology Services (DTS) is planned to better understand the level and types of cyber attacks on the state's network.

In year three the focus will be placed on ensuring local law enforcement and the private sector are fully integrated into the reporting and investigative processes. For the program to be successful, reporting procedures need to be standardized within the state through IC3 so a complete picture can be developed regarding the level and types of cyber crime Utah is experiencing.

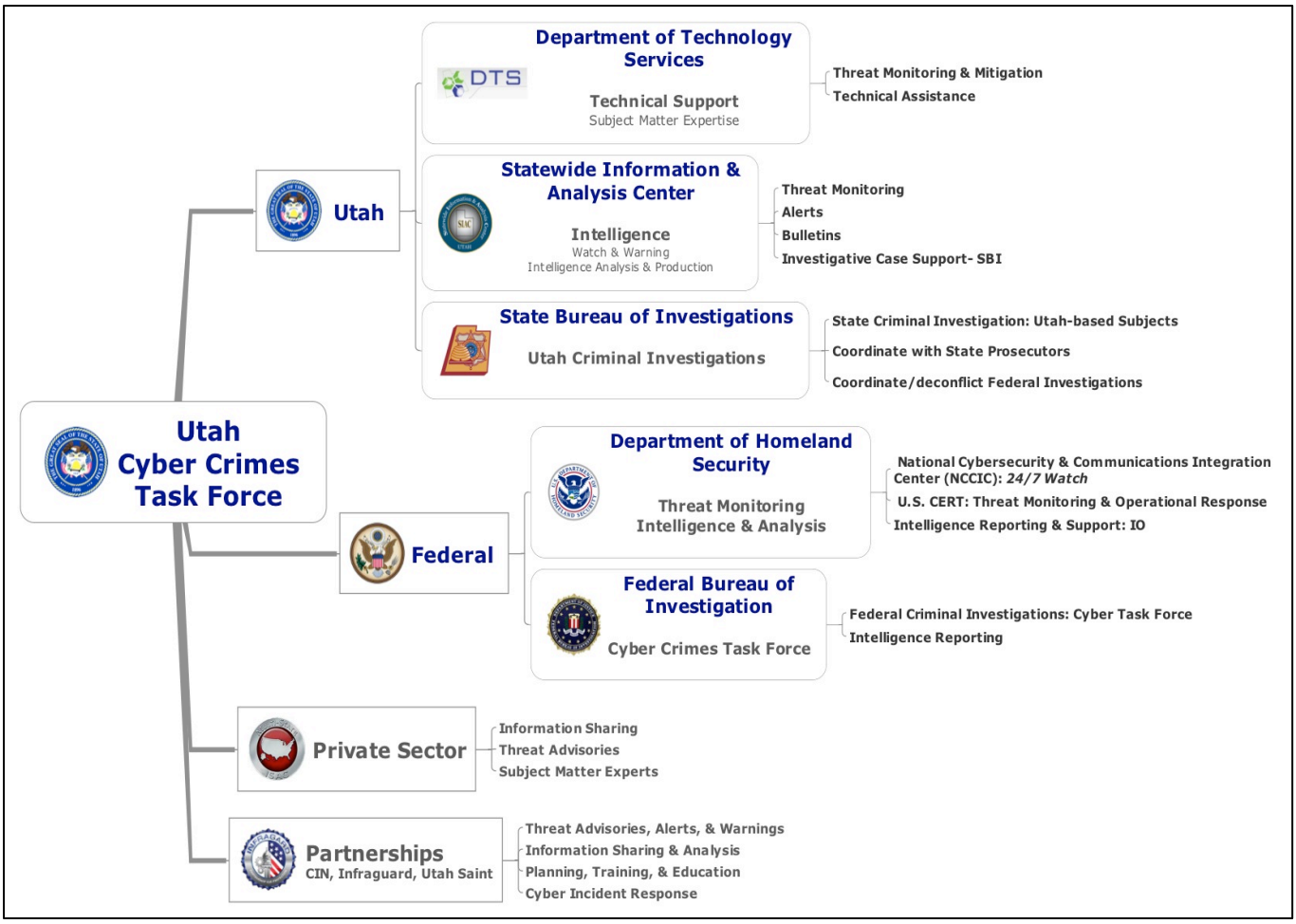
Conclusion

The State of Utah's unified effort to improve situational awareness, share critical intelligence, and investigate computer related crimes will result in an overall increase of cyber security. It is the responsibility of the state to ensure that its infrastructure, partners, and citizens are protected from cyber threats and data breaches. This program is designed to handle the significant issues that continually arise in the cyber landscape.

---

[5] The mission of the High Intensity Drug Trafficking Area (HIDTA) Program is to enhance and coordinate America's drug-control efforts among local, state and Federal law enforcement agencies in order to eliminate or reduce drug trafficking and its harmful consequences in critical regions of the United States. The mission includes coordination efforts to reduce the production, manufacturing, distribution, transportation and chronic use of illegal drugs, as well as the attendant money laundering of drug proceeds.

Utah Statewide Cyber Intelligence Network
Appendix A



Work Flow Structure
Appendix B